世界で起きている政府のインターネット介入

JCA-NET セミナー

2024 年 9 月 21 日

小倉利丸

toshi@jca.apc.org

世界で起きている政府のインターネット介入

インターネットが社会の基幹的なインフラになり、多くの人々がブログや SNS で自由に発信することを日常のコミュニケーション文化として享受するようになっています。インターネットのなかった時代に、世論形成の主要な役割を担ってきたマスメディアが、唯一絶対の情報発信力を独占していました。しかし、現代では、年齢が下がるほどマスメディアの情報に依存する割合が低くなっており、むしろネットの情報が多くの人々を動員できる力を発揮するようになっています。たとえば、ほとんどテレビに出演しないミュージシャンが、オンライン配信やアリーナコンサートで多くの聴衆を集めたり、ネットのインフルエンサーの書き込みが飲食業の集客を左右するなどということはごく当たり前になっています。

こうしたメディア環境の大きな変動は、ネットの世論の力が増すとともに、ガザの戦争にみられるように、「情報戦」としての役割を果すようになってきました。特に選挙や国政に重要な影響を及ぼすような出来事の場合、人々の政治活動の中心を担うのがネットでの情報発信になります。政府もまたネットでの情報発信への様々な規制を通じて世論操作を試みるようになっています。いわゆるグローバルサウスといわれる国々では、反政府運動によるネットでの情報発信を規制する動きが顕著になっています。選挙期間中や、反政府運動の盛り上がりのなかで、インターネットを遮断するなどの行為が起きることはまれではありません。

今回のセミナーでは、政府が介入してインターネットにおける政治活動や言論活動を弾圧したり抑制する事例について、特に選挙や紛争を巡る事例について、JCA-NET がこの間海外の団体とともに、抗議の声明を出したケースを中心に紹介します。

2023年の暴力とインターネット遮断：過去最悪の年となる(Access Now)

https://www.accessnow.org/internet-shutdowns-2023/

2023年は、ほとんどすべての指標において、過去最悪のインターネット遮断の年となった。当局は、暴力、戦争犯罪、民主主義への攻撃、その他の残虐行為を隠し、可能にし、悪化させ、何百万もの人々の人権を押しつぶし、 39カ国で少なくとも283回、意図的にインターネットを遮断した

2023 年の暴力とインターネット遮断：過去最悪の年となる (Access Now)

https://www.accessnow.org/internet-shutdowns-2023/

過去最悪の年

- 政府当局は 39 カ国で少なくとも 283 件のインターネット遮断を実施。 2022 年の 40 カ国 201 件の遮断から 41 %増加
- 戦争。パレスチナ、ミャンマー、スーダン、ウクライナを含む 9 カ国で、戦争当事者が紛争中に少なくとも 74 回インターネットを遮断
- 遮断規模の拡大。インド、イラン、ミャンマー、パレスチナ、ウクライナの数百万人の人々が、少なくとも 211 回の遮断を経験。

  エチオピア、ミャンマー、パキスタンの当局は遮断を長期化

  少なくとも 80 の複数の地域または全国的な規模で遮断
- 新たな加害者たち。ケニア、モザンビーク、ネパール、スリナムが初めてインターネットを遮断。

2023 年の暴力とインターネット遮断：過去最悪の年となる (Access Now)

https://www.accessnow.org/internet-shutdowns-2023/

過去最悪の年 (続き)

- 暴力。暴力行為に関連する遮断が少なくとも 173 件（ 2022 年比 26 %増）、重大な人権侵害が記録された 11 カ国では少なくとも 51 件の遮断
- 縮小する民主主義。抗議行動中に 15 カ国で少なくとも 63 件の遮断。選挙に関連して 5 カ国で少なくとも 5 件の遮断

よいこともいくつか

- 遮断の過去を持つコンゴ民主共和国、ナイジェリア、シエラレオネが #KeepItOn[接続を維持すること] の公約を守る
- 西アフリカ諸国経済共同体（ ECOWAS ）の司法裁判所が再度の遮断に反対の判決を出す
- Freedom Online Coalition（ FOC ）が選挙中にインターネットを遮断しないよう政府に求める声明を発表

2011 年ハーグで開催されたフリーダムオンライン会議で 13 ヶ国によって設立された政府間組織

2023年の暴力とインターネット遮断：過去最悪の年となる (Access Now)

https://www.accessnow.org/internet-shutdowns-2023/

2023年、以下の当局と戦争当事国がインターネットを遮断した。

アルジェリア、アゼルバイジャン、バングラデシュ、ブラジル、中国、キューバ、エチオピア、ガボン、ギニア、インド、インドネシア、イラン、イラク、ヨルダン、ケニア、レバノン、リビア、モーリタニア、モザンビーク、ミャンマー、ネパール、オマーン、パキスタン、パレスチナ、カタール、ロシア、サウジアラビア、セネガル、ソマリランド、スーダン、スリナム、シリア、タンザニア、トルコ、トルクメニスタン、ウガンダ、ウクライナ、アラブ首長国連邦、ベネズエラ。

ベネズエラ

https://www.jca.apc.org/jca-net/ja/node/381

大統領選挙の不正疑惑をめぐる選挙後の抗議運動へのマドゥーロ大統領側の弾圧

選挙後の 1 週間で 2000 人逮捕、 20 人殺害など

7 月 28 日の大統領選挙後、警察、軍、準軍事組織による暴力的な弾圧や、テクノロジーを利用した嫌がらせや迫害

- メッセージングアプリの VenApp などのツールを使用して、反対派の活動を密告させる

  VenApp にはユーザーが国家によって疑わしいとみなされる活動を当局に通報できる機能が組込まれている

- ドクシング

  反体制派の名前、写真、住所などを近隣住民が SNS に曝す

  政府がデモ参加者のプライバシーをネットに暴露する嫌がらせ

- デモのビデオ監視
- パトロール用のドローンを利用した脅迫

ベネズエラ

https://www.jca.apc.org/jca-net/ja/node/381

ベネズエラの NGO 「 Conexión Segura y Libre 」のレポート

ウエッブサイトなどのブロック (国内からサイトにアクセスできなくなる)

- 野党指導者が批判的な論説をウォール・ストリート・ジャーナルに投稿、その後 WJ へのアクセスが遮断
- 現在までに、 62 のメディアが最大手のインターネットサービスプロバイダーによってブロックされ、 86 のドメインが影響を受け、合計 431 のブロックの事象が発生
- 9 つの人権団体のウェブサイトもブロックされ、合計41のブロックが発生

身分証明システムを利用した逮捕、拘束

- 活動家のパスポート無効化や突然の逮捕など
- 身分証明のデータベースがどのように相互リンクされ利用されているのかは、情報開示の制度がないため全くわからない

ケニア

https://www.jca.apc.org/jca-net/ja/node/379

NHKの報道「ケニア 政府への抗議デモ 若者を中心に続く 死者は39人に」

2024年7月3日 1時55分

「東アフリカのケニアで政府の増税案をきっかけに広がった抗議デモは、生活費の高騰にあえぐ若者を中心に各地で続いています。治安部隊との衝突などで、地元の人権団体は、これまでに39人が死亡したとしていて、混乱がさらに深まるおそれも出ています。」

「ルト大統領は、国民の反発を受けて増税案の撤回を発表しましたが、現政権の経済政策に対する国民の不満は根強く、大統領の辞任を求める抗議デモが各地で続いています。」

https://www3.nhk.or.jp/news/html/20240703/k10014499851000.html

政府は公序良俗法 Public Order Actで規定された権限を超えて、抗議者が街頭に出ることを禁止

ケニア

https://www.jca.apc.org/jca-net/ja/node/379

ケニア全国人権委員会（ KNCHR ）の記録

- 治安当局の武力行使で 39 人の死者、 361 人の負傷者、 627 人の逮捕に
- 治安当局によるデモ参加者への拷問に相当する扱い

背景には

長年にわたり平和的なデモ参加者を「暴力的」「犯罪者」としてプロファイリングしてきた。こうしたデータが利用された。

政府は、サイバー空間のさまざまなプラットフォームを通じて計画・実行された国家の安全保障に対する脅威を踏まえ、 ケニア共和国内の 47 の郡を対象に軍や警察の配備を実施

https://www.citizen.digital/news/cs-duale-now-announces-kdf-deployment-to-all-47-counties-n344882

国会議事堂も一時民衆に占拠される

https://www.citizen.digital/news/anti-finance-bill-protestors-trash-parliament-damage-property-n344656

ケニア

https://www.jca.apc.org/jca-net/ja/node/379

政府への抗議はオンラインでも展開された

- 「財政法案反対」、「 #RutoMustGo 」、「 #OccupyChurches 」などのハッシュタグを使い、抗議行動
- X を利用してオンラインで国家的問題について議論
- 逮捕、負傷し、殺害された抗議者のためのクラウドファンディング

オンラインへの弾圧

- X(ツイッター) の活動家を拉致、拘束
- ソーシャルメディア上のコンテンツ制作者、医師、活動家、を含む反対意見に対して脅迫、威嚇、不法な拉致の標的
- ネットワーク接続障害。 6 月 25 日の抗議デモの最盛期に集中的に発生。ソーシャルメディアやメッセージング・アクセスに影響を与え、その影響はウガンダやブルンジにも及んだ。海底ケーブルの切断が原因とされる。
- 携帯電話やパソコンが当局によって不法に没収。
- 被害者たちは勾留中に携帯電話のロック解除を尋問される。

バングラディッシュ

https://www.jca.apc.org/jca-net/ja/node/376

2018 年以来、バングラデシュではインターネットへのアクセスが何度も制限され、ソーシャルメディアやメッセージング・アプリケーションがブロックされてきたが、政府も通信事業者も何の説明もしないままだった。例えば、 2018 年には、道路の安全性をめぐる抗議行動の間、全国的にモバイルインターネットがスローダウンした。 2019 年から 2023 年にかけても、バングラデシュでは抗議行動や反対集会の最中にインターネットが遮断された事例が複数記録されている。

2024 年 7 月上旬以来、公務員採用の 50 %以上をクオータ制 (※) 保持者に保証する制度の廃止を要求する学生デモが、敵意と暴力にさらされながら全国各地で行われている。

※ 独立戦争に従軍した兵士の親族を優先的に公務員として採用する制度、一時期違憲とされたが、その後合憲との判断がだされる

こうした抗議の中、バングラデシュの人々は 2024 年 7 月 18 日夜から全国的なインターネット遮断に見舞われた。

スーダン

https://www.accessnow.org/press-release/access-to-life-saving-telecommunication

軍と即応支援部隊 (準軍事組織の RSF) の間の権力闘争

2019 年、 30 年続いた軍事政権 (バシール政権) が民主化運動で倒れる。民政へに移管プロセスのなかで軍事クーデタなども起きるが、民衆側が民主化闘争を継続してきた。 2023 年に民政移管が実現するはずだったところで軍がこれに抵抗する。この過程で軍内部で、国軍と RSF との権力闘争が激化し、市民がこの内戦に巻き込まれる。

少なくとも1万3,000人の人々が死亡し、世界で最大規模となる900万人以上が国内避難民となるといった悲惨な人道危機に直面。

ここに外国勢力が関与。軍の背後にエジプト、 RSF の背後に UAE （アラブ首長国連邦）やロシアが存在するといわている。

スーダンは原油輸出ルートの紅海に面しており、同時に、レアメタルを産出するチャドや中央アフリカなどのアフリカ内陸部へのアクセスの要衝としてロシア、中国、欧米諸国などが強い関心をもって国軍や RSF と関係をもとうとしてきた。

https://www.nhk.jp/p/catchsekai/ts/KQ2GPZPJWM/blog/bl/pK4Agvr4d1/bp/pazJLKX5Xa/

スーダン

https://www.accessnow.org/press-release/access-to-life-saving-telecommunication

2023 年 4 月に紛争が勃発して以来、即応支援部隊（ RSF ）とスーダン軍（ SAF ）の両方が、敵対派閥が支配する地域における情報の流れを遮断する武器としてインターネット遮断を展開

- RSF ダルフールのインターネットサービスを遮断
- RSF がスーダンの首都ハルツームにあるインターネット・サービス・プロバイダー（ ISP ）のデータセンターを掌握。 2024 年 2 月 2 日に始まり、国内のいくつかの地域でインターネット機能停止が発生
- RSF は配電盤を遮断し、機器に妨害工作を行い、企業がシャットダウン命令に従わない場合はさらに通信インフラを破壊すると脅迫し、遮断が続く。
- 2 月 9 日現在、インターネットはスーダン全土で 1 ヶ月にわたり中断。

  ただし、遮断は国軍による場合もあり情報は錯綜している

CNN: Internet Connection Cut Off, Millions Face Hunger, UN Urges Emergency Aid for Sudan2024.02.09 Fri posted at 10:43 JST

スーダン

https://www.accessnow.org/press-release/access-to-life-saving-telecommunication

双方は一貫して、電気通信インフラに対する標的型攻撃、特定の衛星インターネット機器の輸入・使用禁止を課す

「 2024 年 2 月の全国的な電気通信遮断により、約 3,000 万人のスーダン人が 1 ヶ月以上インターネットや電話を利用できませんでした。スーダン全土で、戦争の惨禍を体験している人々は、家族や愛する人と連絡を取ることができず、離れ離れになっています。スーダン東部ではある程度のサービスが復旧したものの、ダルフール地方やハルツーム、コルドファンの一部など、 Zain 、 MTN 、 Sudani などのネットワークプロバイダーが接続できない地域が依然として広がっています。同じ地域は紛争や飢餓のリスクに最もさらされているため、通信遮断の影響は生命をさらに脅かすことになります。広範な通信手段から遮断された地域では、スターリンクのような衛星接続機器によるサービスしか利用できないところもあります。衛星サービスのコストは民間人のほとんどにとって非常に高額であり、衛星機器の輸入には大きな制限がありますが、国際人道支援組織と現地の対応要員がスーダンで活動を継続するためには、このようなサービスが不可欠であることに変わりはありません。私たちは、このテクノロジーや その他の電気通信システムを紛争当事者が使用することに関して、引き続き重大な懸念がある一方で、（ 2024 年 4 月に発表された）スターリンクの潜在的な遮断は、民間人や、民間人と連絡を取ろうとしている援助組織に過度の影響を与えることになります」 (共同声明：スーダンにおける電気通信の遮断：紛争当事者は、集団的懲罰をやめ、命を救うための電気通信へのアクセスを可能にしなければならない

情報源

Accessnow の #KeepItOn キャンペーン (2024 年選挙運動への政府によるネット遮断などによる介入監視)

https://www.accessnow.org/campaign/2024-elections-and-internet-shutdowns-watch/

情報源

About Tests Data Get Involved Reports Blog Donate

Install OONI Probe

OONI

Open Observatory of Network Interference

Global community measuring Internet censorship since 2012

Test the blocking of websites and apps. Measure the speed and performance of your network.

Install OONI Probe

Testing methodologies →

OONI 2012 年に設立された Open Observatory of Network Interference (OONI) は、非営利のフリーソフトウェア・プロジェクトであり、世界中のインターネット検閲を文書化する分散型の取り組み

https://ooni.org/ 「OONI について」日本語訳 https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/about_ooni/

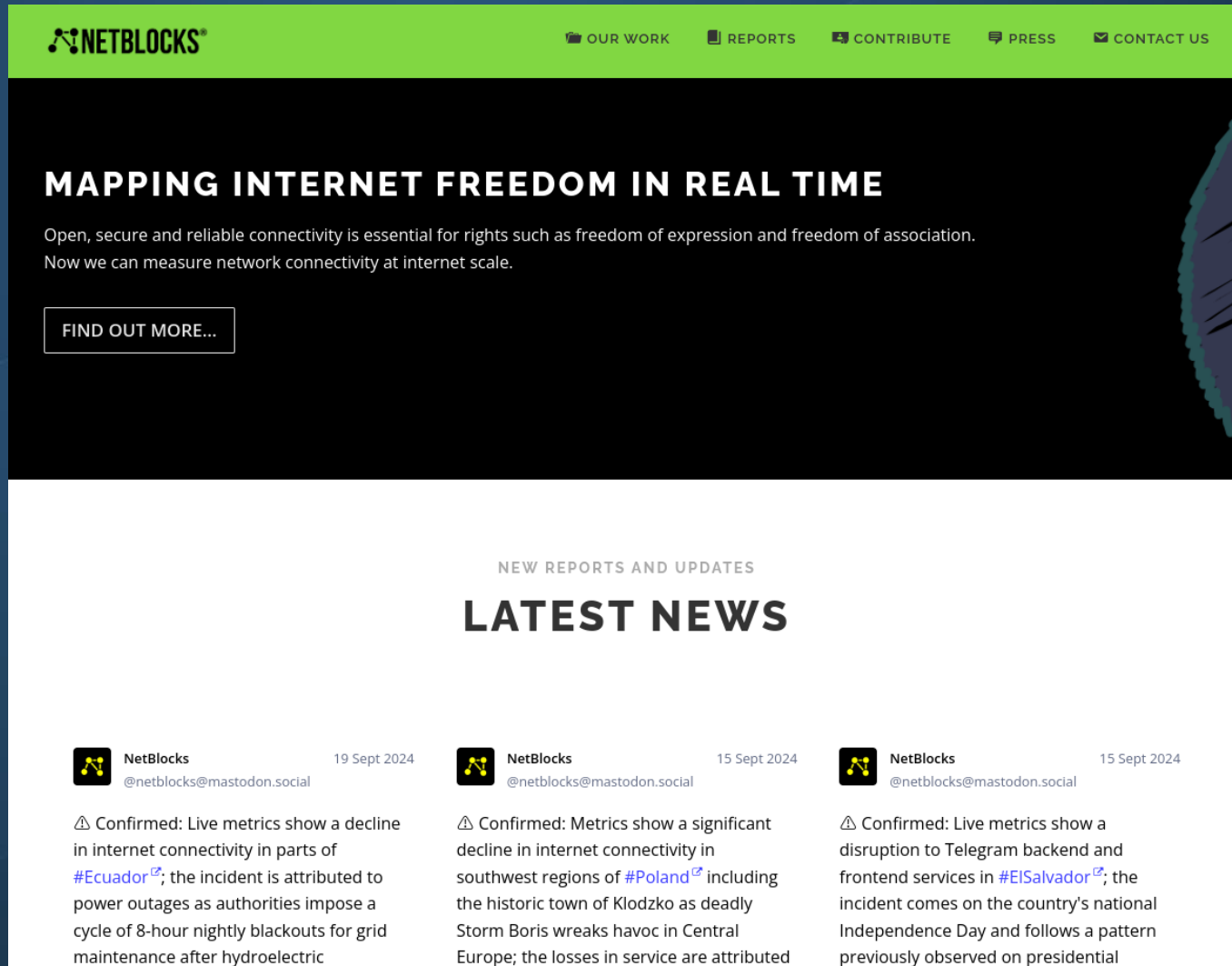
情報源

(ooni.org) カザフスタン TLS MITM 攻撃とニュースメディア、人権、回避ツールサイトのブロッキング

https://cryptpad.fr/pad/#/2/pad/view/o1llGMdvAlXAspm1WCA16bn1Xv0INH3In5rM1Mc7Dg4/

- ニュースサイトのブロック：ロシアTVチャンネル・ツァルグラード（ 2023 年 8 月にカザフスタンでブロックされたと報告されている）の（カザフ語）ウェブサイトなどロシアのニュースメディアウェブサイト
- ウクライナ侵攻後にロシアでブロックされ、現在もロシアでブロックされたままのロシア語の独立系ニュース・サイトである Meduza 、 Kavkaz Center（カザフスタンとロシアの両方でブロックされているチェチェンのインターネット通信社) のブロック
- 国際ニュースメディアウェブサイト Vice Newsカザフスタンでブロックされた唯一の国際ニュースサイト
- Change.org などの署名サイトのブロック
- アムネスティ・インターナショナルのウェブサイトのロシア語版もブロック
- カザフスタンでは 73 の回避ツールウェブサイト (VPN サービスなど) のブロック
- 他方で、 Tor はブロックされていない

ロシアとの緊張を反映しているともいえるが、それだけではない要因もありそうだ。背景となる政治や歴史的な状況などをきちんと把握する必要がある。

情報源

IODA (Internet Outage Detection and Analysis) ほぼリアルタイムでインターネットを監視し、インターネット停止を特定するプロジェクト。米国ジョージア工科大学が運営。米国国土安全保障省、米国務省、 Internet Society などからの財政支援をうけている。

https://ioda.inetintel.cc.gatech.edu

情報源

NEW REPORTS AND UPDATES

LATEST NEWS

NetBlocks 19 Sept 2024
@netblocks@mastodon.social

⚠ Confirmed: Live metrics show a decline in internet connectivity in parts of #Ecuador; the incident is attributed to power outages as authorities impose a cycle of 8-hour nightly blackouts for grid maintenance after hydroelectric

NetBlocks 15 Sept 2024
@netblocks@mastodon.social

⚠ Confirmed: Metrics show a significant decline in internet connectivity in southwest regions of #Poland including the historic town of Klodzko as deadly Storm Boris wreaks havoc in Central Europe; the losses in service are attributed

NetBlocks 15 Sept 2024
@netblocks@mastodon.social

⚠ Confirmed: Live metrics show a disruption to Telegram backend and frontend services in #ElSalvador; the incident comes on the country's national Independence Day and follows a pattern previously observed on presidential

Netblocks は、 人権活動家でもある Alp Tokerがロンドンに拠点を置いて運営。ネットの遮断などを監視している。 https://netblocks.org https://mastodon.social/@netblocks

パレスチナ人のデジタルの権利、ジェノサイド、そしてビッ グテックの説明責任

https://www.jca.apc.org/jca-net/sites/default/files/2024-09/7amleh_Palestinian%20Digital%20Rights%20ja.pdf

この報告書では、人権侵害の実行と悪化にテクノロジーが広く使用されていることを強調している。イスラエル政府は、パレスチナ人を標的にするために人工知能を活用しており、テクノロジー企業は、検閲を容易にし、情報を隠蔽し、間接的にガザで進行中のジェノサイドでイスラエル政府の取り組みに重要な役割を果たしている。この報告は、１年間にわたるパレスチナ人のデジタル上の権利侵害をまとめ、分析し、デジタル上の権利保護のための迅速な行動と、ジェノサイドを防ぐためのテクノロジーポリシーの説明責任のメカニズム開発の緊急性を強調している。

この報告書は、パレスチナ人の声やパレスチナ支持派のコンテンツを組織的に検閲することで、ジェノサイドの最中にデジタル上の権利を侵害するデジタルプラットフォームの役割を検証している。これらの侵害は、パレスチナ人ジャーナリストやコンテンツ制作者のソーシャルメディアアカウントに対する差別的なポリシーや制限によって加速されている。

パレスチナ人のデジタルの権利、ジェノサイド、そしてビッ グテックの説明責任

https://www.jca.apc.org/jca-net/sites/default/files/2024-09/7amleh_Palestinian%20Digital%20Rights%20ja.pdf

2023 年 10 月 7 日から 2024 年 9 月までの間に、 Meta や X などの主要なプラットフォーム上で 5100 件以上のデジタル検閲と有害なコンテンツの拡散を記録した。さらに、偽情報キャンペーンのより一層の広がりがみられ、表現の自由、情報への権利、そしてセキュリティへの権利を損なうことが示された。ガザの 200 万人以上の人々が飢餓の脅威に直面する中、偽情報がパレスチナ人に対する集団的処罰を正当化し、人道支援の取り組みを妨げるために使用されている。

この報告書の調査により、一部のオンラインプラットフォームが有害な広告コンテンツから利潤を得ていることが明らかになった。例えば、 Meta が所有する Facebook は、個人暗殺を扇動し、パレスチナ人の西岸地区からヨルダンへの強制退去を主張するターゲット広告を掲載していた。さらに、 YouTube の広告ポリシーは人権基準に準拠していないことが判明した。イスラエル外務省は、 YouTube 上でガザ地区に対する継続中の戦争に関する広告を推進し、2023 年 10 月 7 日以降 2 週間で 710 万ドルの予算を投じ、フランス、ドイツ、英国の視聴者にそのイデオロギーを拡散させた。こうした広告は、プラットフォーム自身のポリシーに違反している。

パレスチナ人のデジタルの権利、ジェノサイド、そしてビッ グテックの説明責任

https://www.jca.apc.org/jca-net/sites/default/files/2024-09/7amleh_Palestinian%20Digital%20Rights%20ja.pdf

Palestinian Digital Rights, Genocide, and Big Tech Accountability

ガザ地区をめぐる状況において、人工知能、データ収集、監視、自動化がどのように相互に結びつき、パレスチナ人のデジタルの権利に悪影響を及ぼしているのかについても掘り下げている。そして、大手テクノロジー企業に説明責任を果たさせることの必要性と、国際犯罪や人権侵害にこれらのテクノロジーが使用されるのを防ぐための厳格な規制を確立することの重要性を強調している。イスラエルがガザでの軍事行動中に、違法な戦争戦術としてインターネットとワイヤレス通信の遮断を使用し、パレスチナ人の重要なインターネットと通信サービスを妨害し、重要インフラを標的にしたことも記録されている。本報告は、この戦術の歴史的背景と国際人道法違反について取り上げ、遮断がガザでの深刻な人権侵害を記録する上での大きな障害となっていることを示している。

本報告は、パレスチナ人の人権およびデジタル上の権利保護を進めるために必要な条件として、即時停戦を求めている。また、パレスチナ人および世界中でパレスチナの人権を擁護する人々に対するオンライン上での組織的かつ意図的な差別的ポリシーや慣行を終わらせるために、官民のアクターが積極的に協力する必要があることを強調している。報告書はまた、大手テクノロジー企業、オンラインプラットフォーム、通信会社、国際的な利害関係者に対する一連の提言も提起している。

私たちの教訓として

政府による遮断やアクセス困難には様々な局面がある

- 国全体のネットワークを遮断する
- 特定のサービス (SNS など) を遮断する
- 特定の情報源へのアクセスを遮断する
- 通信速度を落して繋りにくくする

人々を監視するための情報収集

- 反体制派の動静把握
- 逮捕、家宅捜索、拷問などの手法と押収したコンピュータや通信機器からの情報取得の組み合わせ
- SNS などを利用した密告制度
- 既存のデータベースを弾圧や治安対策などに転用

私たちの教訓として

どのような状況で政府の介入が深刻化するのか

- 現政権の危機を背景とした選挙
- 戦争 (内戦) 状態
- 反政府運動の高揚

法制度はどのように機能しているのか

- 憲法や国際人権法などを政府が事実上無視する
- 監視や弾圧に都合のよい法制度が制定される

通信事業者はどう対応しているのか

- ユーザーの人権よりも政府の意向を優先する

私たちの教訓として

政府の介入への抵抗

- 国内の人権団体などによる抵抗
- 国際的な連携による支援
- 遮断や監視を回避する技術的なノウハウの共有

日本の現状への教訓

- 政府が保有している個人データは政府の政権の危機などに直面したときは、治安監視の手段になる。マナンバーのデータ、保健医療のデータなどが逸脱した利用をされうる。
- 大手の通信事業者は、どこの国でも政府寄りの姿勢をとりやすい。通信事業者と政府が一体となってユーザーを監視する可能性があることを念頭に置くべき。
- プライバシーツールの利用をライフスタイルにすることが重要になる。